# ESET ENDPOINT SECURITY

## PARA ANDROID

Manual de instalação e Guia do usuário

Clique aqui para fazer download da versão mais recente deste documento

# Índice


1. Instalação do ESET Endpoint Security....3
1.1 Instalação ....3
1.2 Desinstalação....4
2. Ativação do produto....4
3. Antivírus....4
4. Controle USSD....6
5. Antispam....7
6. Antifurto....7
7. Auditoria de segurança....9
8. Administração remota....9
9. Atualização....11
10. Senha....11
11. Solução de problemas e suporte....11
11.1 Solução de problemas....11
11.2 Suporte técnico....12


ESET **ENDPOINT SECURITY**


**Copyright ©2012 da ESET, spol. s r.o.**

O ESET Endpoint Security foi desenvolvido pela ESET, spol. s r.o. Para obter mais informações, acesse www.eset.com. Todos os direitos reservados. Nenhuma parte desta documentação pode ser reproduzida, armazenada em um sistema de recuperação ou transmitida de qualquer forma ou por qualquer meio, eletrônico, mecânico, fotocópia, gravação, digitalização ou de outra natureza, sem a permissão por escrito do autor.

A ESET, spol. s r.o. reserva-se o direito de alterar qualquer um dos aplicativos de software descritos sem prévio aviso.



Atendimento ao Cliente: www.eset.com/support

REV. 17. 12. 2012

# 1. Instalação do ESET Endpoint Security

Para instalar o ESET Endpoint Security para Android, seu dispositivo móvel deve atender aos seguintes requisitos do sistema:

| | Requisitos mínimos do sistema |
|---|---|
| Sistema operacional | Android 2.1 (Eclair) e posterior |
| CPU | 600 MHz |
| RAM | 256 MB |
| Espaço livre de armazenamento interno | 5 MB |

**OBSERVAÇÃO:** Alguns recursos (por ex. Antispam e Antifurto) não estão disponíveis em Android 3.0/ tablets que não suportem chamadas e mensagens. Veja mais detalhes neste artigo da base de conhecimento (é possível que não esteja disponível em seu idioma).

## 1.1 Instalação

Para instalar o ESET Endpoint Security, use um dos seguintes métodos:

- Faça download do arquivo de instalação do ESET Endpoint Security *(ees.apk)* no site da ESET por meio da leitura do código QR a seguir com um aplicativo como QR Droid ou Barcode Scanner:

- Faça download do arquivo *ees.apk* em seu computador pelo site da ESET. Copie o arquivo para o seu dispositivo via Bluetooth ou USB. Toque no ícone do Iniciador na tela inicial do Android ou vá para **Início** > **Menu** e toque em **Configurações** > **Aplicativos.** Certifique-se de que a opção **Fontes desconhecidas** esteja marcada. Localize o arquivo *ees.apk* usando um aplicativo como o ASTRO File Manager ou o ES File Explorer. Abra o arquivo e toque em **Instalar**. Depois que o aplicativo for instalado, toque em **Abrir**.

- Caso deseje instalar e ativar o ESET Endpoint Security em vários dispositivos, crie um arquivo xml de configuração no ESET Configuration Editor.

  Abra o ESET Configuration Editor no ERA Console ( **Ferramentas** > ESET Configuration Editor) ou clique em **Iniciar** > **Todos os Programas** > **ESET** > ESET Remote Administrator **Console >** ESET Configuration Editor. Na árvore à esquerda, selecione **Dispositivos móveis** > **Endpoint Security for Android** > **Atualizar** > **Configurações** > **Nome de usuário**. Informe seu nome de usuário (dados de licença recebidos da ESET após a compra do produto) no campo **Valor** à direita e clique em **Avançar**. Clique em **Configurar senha** e informe a senha. Clique em **OK** para confirmar. Você também pode definir configurações adicionais (por exemplo, configurações de Administração Remota ou Antivírus) que deseja aplicar a todos os dispositivos móveis de pontos de extremidade usando o ESET Configuration Editor. Depois de concluir as configurações, clique em **Arquivo** > **Salvar** (ou pressione Ctrl+S) e salve o arquivo como *settings.xml*.

  Copie o arquivo que acabou de salvar na pasta raiz de seu cartão SD *(/mnt/sdcard)*, juntamente com o arquivo de instalação do ESET Endpoint Security *ees.apk* (disponível aqui). Abra o arquivo *ees.apk* usando um aplicativo como o ASTRO File Manager ou o ES File Explorer e toque em **Instalar**. Depois que a instalação for concluída, toque em **Abrir**. O ESET Endpoint Security será ativado automaticamente com o nome de usuário e senha salvos no arquivo *settings.xml*.

***Aviso:*** O ESET Endpoint Security deve ser instalado no armazenamento interno do dispositivo. Alguns celulares permitem que os usuários instalem aplicativos no cartão SD. Se você instalar o ESET Endpoint Security no cartão SD, a Proteção em tempo real, o Antispam e o Antifurto não funcionarão.

Após a instalação, ative o ESET Endpoint Security seguindo as etapas descritas na seção Ativação do produto 4.

### 1.2 Desinstalação

Para desinstalar o ESET Endpoint Security do dispositivo, use o **Assistente de desinstalação**, que pode ser acessado no menu principal do ESET Endpoint Security ou siga as etapas abaixo:

1. Toque no ícone do iniciador na tela inicial do Android (ou vá para **Início** > **Menu**) e toque em **Configurações** > **Local e segurança** > **Selecionar administradores de dispositivo**, desmarque **ESET Security** e toque em **Desativar**. Quando solicitado, digite sua senha do ESET Endpoint Security. Se você não tiver definido o ESET Endpoint Security como o Administrador do dispositivo, ignore esta etapa.
2. Volte para **Configurações** e toque em **Aplicativos** > **Gerenciar aplicativos** > **ESET Security** > **Desinstalar** .

O ESET Endpoint Security e a pasta de quarentena serão removidos permanentemente do seu dispositivo móvel.

## 2. Ativação do produto

Após a instalação, o ESET Endpoint Security deve ser ativado. Toque em **Ativar agora** no menu principal do ESET Endpoint Security.

**Ativar utilizando um Usuário e Senha** - digite o usuário e a senha (dados de licença recebidos da ESET após a aquisição do produto) nos campos adequados.

A ativação é valida por determinado período de tempo. Depois que a ativação expirar, você deverá renovar a licença do programa (o programa notificará sobre essa necessidade com antecedência).

**OBSERVAÇÃO:** Durante a ativação, o dispositivo precisa estar conectado à Internet. Será feito o download de uma pequena quantidade de dados.

Por padrão, o ESET Endpoint Security é instalado no idioma definido em seu telefone como local do sistema (nas configurações de idioma e teclado). Para alterar o idioma da interface de usuário do aplicativo, toque em **Idioma** no menu principal do ESET Endpoint Security e selecione o idioma desejado.

## 3. Antivírus

#### Rastrear dispositivo

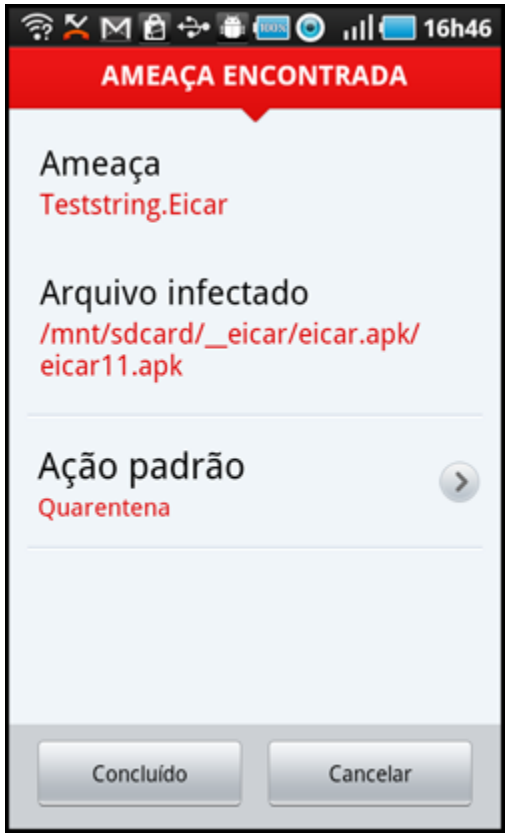
A opção **Rastrear dispositivo** pode ser usada para verificar se há infiltrações no dispositivo móvel.

Alguns tipos de arquivo predefinidos são rastreados por padrão. Um rastreamento completo do dispositivo verifica a memória, os processos em execução, as bibliotecas de links dependentes e arquivos que fazem parte dos armazenamentos interno e removível. Um breve resumo do rastreamento será exibido após a conclusão do processo (ou seja, o número de arquivos infectados, o número de arquivos rastreados, a duração do rastreamento etc.).

Para anular o rastreamento em andamento, toque em **Cancelar**.

#### Rastrear pasta

Para rastrear pastas específicas do dispositivo, toque em **Rastrear pasta**. Localize as pastas que deseja rastrear, toque nas caixas de seleção correspondentes na coluna direita e depois em **Rastrear**.




**Ameaça detectada pelo** ESET Endpoint Security

### Rastrear logs

A seção **Rastrear logs** traz logs que fornecem dados abrangentes sobre as tarefas de rastreamento concluídas. Os logs são criados sempre que um rastreamento é acionado manualmente (Sob demanda) ou quando uma infiltração é detectada pelo Rastreamento em tempo real.

Cada log contém:

- data e hora do evento
- número de arquivos rastreados
- número de arquivos infectados
- caminho completo dos arquivos infectados
- duração do rastreamento
- ações executadas ou erros ocorridos durante o rastreamento.

### Quarentena

A principal tarefa da quarentena é armazenar os arquivos infectados de maneira segura. Os arquivos devem ser colocados em quarentena se não for possível limpá-los, se não for seguro nem aconselhável excluí-los ou se tiverem sido falsamente detectados pelo ESET Endpoint Security.

É possível consultar os arquivos em quarentena em um log que discrimina o nome e o local original do arquivo infectado, bem como a data e a hora da quarentena.

Para restaurar um arquivo em quarentena para seu local original, toque nele e selecione **Restaurar**. Não é recomendável utilizar essa opção.

Para remover um arquivo em quarentena permanentemente do dispositivo, toque nele e selecione **Excluir**. Para remover todos os arquivos em quarentena, pressione o botão **MENU** e toque em **Excluir tudo**.

### Configurações

As configurações **Sob demanda** permitem alterar os parâmetros de um rastreamento acionado manualmente (Sob demanda).

A opção **Exibir janela de diálogo de alerta** exibe notificações de alerta sobre ameaças sempre que uma nova ameaça é detectada pelo scanner sob demanda.

Para rastrear todos os aplicativos (os arquivos *.apk*) instalados no dispositivo, selecione a opção **Rastrear aplicativos**.

A **Proteção proativa** é um método de detecção por algoritmos que analisa o código e procura atividades tipicamente executadas por vírus. A principal vantagem desse método é a possibilidade de identificar software malicioso que ainda não foi registrado no banco de dados atual de assinatura de vírus. O rastreamento levará mais tempo para ser concluído se a Proteção proativa estiver ativada.

A opção **Nível de rastreamento em arquivos compactados** permite especificar o número de camadas em arquivos compactados (arquivos *.zip*) a ser rastreado. Quanto mais alto for o número, mais profundo será o rastreamento.

A opção **Logs armazenados** permite definir o número máximo de logs que poderão ser armazenados na seção **Rastrear logs** 5.

É possível especificar a **Ação padrão** que será executada automaticamente quando arquivos infectados forem detectados. As seguintes ações podem ser definidas como padrão:

- **Ignorar** - nenhuma ação é executada no arquivo infectado (não é recomendável selecionar esta opção)
- **Excluir** - o arquivo infectado é removido
- **Quarentena** (padrão) - o arquivo infectado é colocado em **quarentena** 5.

As configurações **Extensões** mostram os tipos de arquivo mais comuns expostos a infecções na plataforma Android. Selecione os tipos de arquivo que deseja rastrear ou desmarque as extensões que deseja excluir do rastreamento. Essas configurações aplicam-se aos rastreamentos sob demanda e em tempo real:

- **Rastrear por extensões** - se você selecionar esta opção, somente arquivos com as extensões especificadas serão rastreados, o que acelera o processo de rastreamento. Recomendamos que você desative essa funcionalidade de vez em quando para permitir que o ESET Endpoint Security rastreie todos os tipos de ameaça possíveis, incluindo infiltrações ocultas por extensões de arquivo falsas.
- **DEX (Arquivo de código de aplicações)** - formato de arquivo executável que contém código compilado programado para o sistema operacional Android
- **SO (Bibliotecas)** - bibliotecas compartilhadas salvas em locais designados no sistema de arquivos e vinculadas por programas que usam suas funções
- **Arquivos (arquivos compactados)** - arquivos compactados por meio da compactação em Zip
- **Outros** - outros tipos de arquivo conhecidos.

Nas configurações **Tempo real**, é possível configurar os parâmetros de rastreamento em tempo real. O scanner em tempo real verifica os arquivos à medida que você interage com eles. Ele rastreia automaticamente a pasta *Download* no cartão SD, os arquivos de instalação *.apk* e os arquivos no cartão SD quando ele é montado (se a opção **Rastrear cartão SD montado** estiver ativada). O scanner em tempo real é carregado automaticamente com a inicialização do sistema.

- **Proteção em tempo real** - se ativada (padrão), o scanner em tempo real é executado em segundo plano.
- **Exibir janela de diálogo de alerta** - exibe notificações de alerta sobre ameaças sempre que uma nova ameaça é detectada pelo scanner em tempo real.
- **Rastrear cartão SD montado** - rastreia os arquivos antes de serem abertos ou salvos no cartão SD.
- **Proteção proativa** - selecione esta opção para aplicar técnicas heurísticas de rastreamento. A heurística identifica proativamente novos malwares que ainda não foram registrados no banco de dados de assinatura de vírus analisando o código e reconhecendo atividades tipicamente executadas por vírus. O rastreamento levará mais tempo para ser concluído se a Proteção proativa estiver ativada.
- **Nível de rastreamento em arquivos compactados** - esta opção permite especificar o nível de arquivos compactados (arquivos *.zip*) a ser rastreado. Quanto mais alto for o número, mais profundo será o rastreamento.
- **Ação padrão** - é possível especificar a ação padrão que será executada automaticamente quando arquivos infectados forem detectados pelo scanner em tempo real. Se você selecionar **Ignorar**, nenhuma ação será executada no arquivo infectado (não é recomendável selecionar esta opção). Se selecionar **Excluir**, o arquivo infectado será removido. Se selecionar **Quarentena**, o arquivo infectado será colocado em **quarentena** 5.

O ESET Endpoint Security exibe seu ícone de notificação no canto superior esquerdo da tela (barra de status do Android). Se você não deseja que esse ícone seja exibido, vá para o menu principal do ESET Endpoint Security, pressione o botão **MENU**, toque em **Notificações** e desmarque a opção **Mostrar ícone na barra de status**. Isso não desativará o ícone vermelho de aviso com ponto de exclamação que notifica o usuário sobre riscos de segurança (por exemplo, com o rastreamento de vírus em tempo real desativado, a correspondência de SIM desativada etc.).

## 4. Controle USSD

A versão mais recente do ESET Endpoint Security (1.2.103 e posteriores) protege seu dispositivo Android de limpeza remota e outros ataques USSD. Os códigos USSD (Unstructured Supplementary Service Data, Dados de serviços complementares não estruturados) podem ser executados por mensagens de texto mal-intencionadas, códigos QR ou links de URL.

Se você receber uma notificação de que uma nova versão do ESET Endpoint Security está disponível para download, a ESET recomenda que você a instale assim que possível.

O Controle USSD não está acessível do menu principal; ele é executado em segundo plano e somente o notifica quando um comando USSD é executado. Para verificar com segurança seu dispositivo quanto à vulnerabilidade a USSD, siga as instruções descritas nas etapas 4 a 6 deste artigo da base de conhecimento.

# 5. Antispam

O módulo **Antispam** bloqueia mensagens SMS/MMS recebidas e chamadas recebidas/realizadas de acordo com as suas regras.

Mensagens indesejadas geralmente incluem anúncios de operadoras ou mensagens de usuários desconhecidos ou indeterminados. O termo *bloquear contatos* refere-se à transferência automática de uma mensagem recebida para a seção **Logs de spam** 7. Nenhuma notificação é exibida quando uma mensagem recebida é bloqueada. A vantagem é que o usuário não é incomodado pelas informações indesejadas, mas, ao mesmo tempo, pode consultar os logs para procurar mensagens que possam ter sido bloqueadas por engano.

Para adicionar uma nova regra antispam, toque em **Permissões de chamada e SMS** > **Adicionar nova**. Insira o número de telefone que deseja bloquear ou toque no botão **+** para selecionar o número a partir da lista de contatos. Personalize a regra permitindo ou bloqueando mensagens e chamadas e toque em **Concluído**.

Para editar ou remover uma entrada de regra existente, toque e segure-a e selecione a ação desejada. Para remover todas as regras antispam, pressione o botão **MENU** e toque em **Remover tudo**.

**OBSERVAÇÃO:** O número de telefone deve incluir o código de discagem internacional seguido pelo número propriamente dito (por exemplo, +16101001OO).

**Lista de permissões antispam**

**Configurações**

**Bloquear chamadas anônimas** - ative esta opção para bloquear ligações de pessoas que ocultaram seu número de telefone deliberadamente pelo recurso de restrição de identificação da linha chamadora.

**Bloquear contatos da agenda** - use esta opção para bloquear mensagens e chamadas de contatos incluídos na sua lista de contatos.

**Bloquear números desconhecidos** - bloqueia mensagens e chamadas de contatos que não estão incluídos na sua lista de contatos. Você pode usar essa opção para bloquear chamadas indesejadas (por exemplo, ligações de telemarketing) ou para evitar que crianças disquem números desconhecidos. Para evitar isso, é recomendável proteger suas configurações de antispam com **senha** 11.

Na seção **Logs de spam**, você pode consultar as chamadas e mensagens bloqueadas pelo módulo Antispam. Cada log contém o nome do evento, o número de telefone correspondente e a data e a hora do evento. As mensagens SMS bloqueadas preservam o corpo da mensagem.

# 6. Antifurto

A funcionalidade **Antifurto** protege seu celular contra acesso não autorizado.

Se você perder o telefone ou se alguém roubá-lo e trocar o cartão SIM por um novo (não confiável), o telefone será bloqueado automaticamente pelo ESET Endpoint Security. Um SMS de alerta será enviado para o número ou números de telefone definidos pelo usuário. Essa mensagem incluirá o número de telefone do cartão SIM inserido no momento, o número IMSI (International Mobile Subscriber Identity, identidade internacional de assinante móvel) e o número IMEI (International Mobile Equipment Identity, identidade internacional de equipamento móvel) do telefone. O usuário não autorizado não terá conhecimento do envio dessa mensagem, pois ela é automaticamente excluída das sequências de **mensagens**. Você também pode solicitar coordenadas de GPS do celular perdido ou apagar remotamente todos os dados armazenados no dispositivo.

**Cartões SIM confiáveis**

Esta funcionalidade não está disponível em dispositivos sem cartão SIM (tablets e telefones CDMA).

Para salvar o cartão SIM inserido no celular como confiável, toque no botão **Adicionar**. Se você usa mais de um cartão SIM, é recomendável diferenciar cada um alterando o **Apelido do cartão SIM** (por exemplo *Comercial*, *Residencial* etc.).

Para **Editar** ou **Remover** uma entrada de SIM existente, toque e segure-a e selecione a ação desejada. Para remover todas as entradas da lista, pressione o botão **MENU** e toque em **Remover tudo**.

**Contatos do administrador**

Na lista **Contatos do administrador**, **adicione** os números de telefone das pessoas que receberão um SMS de alerta se um cartão SIM não confiável for inserido no seu dispositivo. Insira um nome no campo **Nome do contato** e o número de telefone no campo **Número de telefone** ou toque no botão **+** para selecionar o contato a partir da lista de contatos. Caso o contato tenha mais de um número de telefone, o SMS de alerta será enviado para todos os números.

Para **Editar** ou **Remover** uma entrada existente, toque e segure-a e selecione a ação desejada. Para remover todas as entradas da lista, pressione o botão **MENU** e toque em **Remover tudo**.

**OBSERVAÇÃO:** O número de telefone deve incluir o código de discagem internacional seguido pelo número propriamente dito (por exemplo, +16101001OO).

**Configurações**

Caso não deseje usar a correspondência de SIM, selecione a opção **Ignorar correspondência de SIM**. Isso desativará avisos vermelhos *Risco de segurança!* (*A correspondência de SIM está desativada* e *Nenhum SIM confiável definido*) no menu principal do ESET Endpoint Security. A opção Ignorar correspondência de SIM fica acinzentada em dispositivos com base em CDMA.

Para ativar a verificação automática do cartão SIM inserido (e o envio do SMS de alerta), selecione a opção **Ativar correspondência de SIM**.

No campo **Texto de Alerta SMS**, é possível alterar a mensagem que será enviada ao(s) número(s) de telefone predefinido(s) se um cartão SIM não confiável for inserido no seu dispositivo. Também é possível informar outro e-mail ou um número de contato alternativo.

**Comandos por SMS**

Os comandos remotos por SMS (exclusão dos dados, bloqueio e localização) só funcionarão se a opção **Permitir comandos por SMS** estiver selecionada.

A opção **Permitir senha redefinida de SMS** permite redefinir a senha de segurança por meio do envio de um SMS a partir do celular salvo nos **Contatos do administrador** do seu número de telefone. Esse SMS deve ter o seguinte formato:
*eset remote reset*

Se você perder seu telefone e desejar bloqueá-lo, envie um SMS de bloqueio remoto para seu celular a partir de qualquer outro dispositivo móvel no seguinte formato:
*eset lock senha*
Substitua *senha* pela sua própria senha (definida na seção **Senha** 11). Nenhum usuário autorizado conseguirá usar seu telefone, pois será necessário inserir a senha que você criou.

Para solicitar as coordenadas de GPS do seu celular, envie um SMS de localização remota para seu celular ou para o número de telefone do usuário não autorizado (o procedimento dependerá se o cartão SIM já tiver sido substituído ou não):
*eset find senha*
Você receberá um SMS com as coordenadas de GPS e um link para o Google Maps mostrando a localização exata de seu celular. Para que seja possível receber as coordenadas de GPS, o módulo GPS do telefone deverá ter sido previamente ativado.

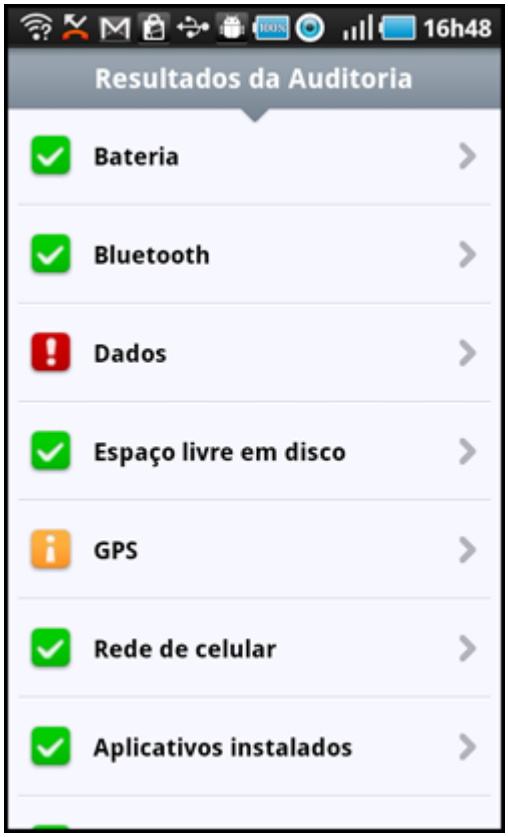
Para apagar todos os dados armazenados no seu dispositivo e todas as mídias removíveis inseridas no momento, envie um SMS de Limpeza Remota:
*eset wipe senha*
Todos os contatos, mensagens, e-mails, aplicativos instalados, sua conta do Google e o conteúdo do cartão SIM serão permanentemente apagados do dispositivo. Se o ESET Endpoint Security não estiver definido como o Administrador do dispositivo, somente os contatos, as mensagens e o conteúdo do cartão SD serão apagados.

**OBSERVAÇÃO:** A senha diferencia maiúsculas e minúsculas. Insira a senha exatamente como ela foi definida na seção Senha.

# 7. Auditoria de segurança

A **Auditoria de segurança** verifica o status do telefone em termos de nível da bateria, status do Bluetooth, espaço livre em disco, etc.

Para executar uma auditoria de segurança manualmente, toque em **Auditoria**. Um relatório detalhado será exibido.




**Resultados da auditoria de segurança**

Um tique verde ao lado de cada item indica que o valor é superior ao limite mínimo ou que o item não representa um risco de segurança.

Um ícone amarelo significa que pelo menos um dos itens está abaixo do limite mínimo ou que o item pode representar um risco de segurança. Toque no item para ver os resultados detalhados.

Um ponto de exclamação vermelho indica que o item está abaixo do limite mínimo ou que representa um risco de segurança e deve ser corrigido.

Para corrigir o status do item realçado em vermelho, toque no item e depois em **Sim** para confirmar.

**Configurações**

A auditoria de segurança é programada por padrão para ser executada a cada 24 horas. Para desativar a auditoria periódica, desmarque a opção **Auditoria periódica**.

Se a opção **Corrigir automaticamente** estiver ativada, o ESET Endpoint Security tentará corrigir os itens em risco automaticamente (por exemplo, o status do Bluetooth) sem a interação do usuário. Essa opção só se aplica à auditoria periódica (programada).

A opção **Logs armazenados** permite definir o número máximo de logs que poderão ser armazenados na seção **Logs da auditoria**.

A opção **Período de auditoria** permite definir com que frequência a auditoria periódica (programada) será executada.

Para ajustar o valor do limite em que o espaço livre em disco e o nível da bateria são considerados baixos, use as opções **Limite de espaço livre em disco** e **Limite de nível de bateria**.

Na guia **Itens para auditoria**, selecione os itens que serão verificados durante a auditoria periódica (programada).

A seção **Logs da auditoria** contém logs que fornecem dados completos sobre as auditorias periódicas e manuais realizadas. Cada log contém a hora e a data do evento e resultados detalhados de cada item.

O **Gerenciador de tarefas** apresenta uma visão geral de todos os processos, serviços e tarefas em execução no dispositivo. O ESET Endpoint Security permite interromper processos, serviços e tarefas que não estiverem sendo executados pelo sistema. Eles são indicados por um ícone vermelho (**x**).

# 8. Administração remota

O ESET Remote Administrator (ERA) permite gerenciar o ESET Endpoint Security em um ambiente de rede diretamente de um local centralizado.

Os administradores podem executar as seguintes ações remotamente:

- criar uma tarefa de configuração no ERA e distribuir as configurações para o ESET Endpoint Security,
- acionar o rastreamento sob demanda,
- instalar atualizações do banco de dados de assinatura de vírus,
- verificar arquivos de log,
- enviar mensagens administrativas para dispositivos móveis.

O uso do ERA não só aumenta o nível de segurança, mas também facilita a administração de todos os produtos da ESET instalados nos dispositivos móveis e estações de trabalho clientes. Os dispositivos móveis com ESET Endpoint Security podem se conectar ao ERA usando qualquer tipo de conexão com a internet - LAN, WLAN, rede celular (3G, HSDPA, GPRS), etc. - desde que seja uma conexão com a internet regular (sem um proxy, firewall, etc.) e ambos os pontos de extremidade estejam configurados corretamente. Ao se conectar ao ERA por uma rede celular, uma conexão bem-sucedida dependerá do provedor GSM e exigirá uma conexão com a internet completa. Por exemplo, se somente a navegação http na web for permitida usando a porta 80, a conexão falhará pois a porta 2222 é necessária para comunicação com o servidor ERA.

**Configurações**

As opções de configuração da administração remota estão disponíveis no menu principal do ESET Endpoint Security. Toque em **Administração remota** > **Configurações**.

Para ativar a administração remota, selecione a opção **Conectar-se ao servidor de administração remota**.

**Intervalo entre as conexões com o servidor** - esta opção determina a frequência com que o ESET Endpoint Security tentará se conectar ao ERA Server para enviar os dados.

**Servidor primário**, **Servidor secundário** - em geral, apenas o servidor primário precisa ser configurado. Se você estiver executando vários servidores ERA na rede, poderá optar por adicionar uma conexão com um ERA Server secundário. Ele servirá como a solução de fallback. Se o servidor primário ficar inacessível, o ESET Endpoint Security automaticamente estabelecerá contato com o ERA Server secundário. Simultaneamente, ele tentará restabelecer a conexão com o servidor primário. Depois que a conexão ficar ativa novamente, o ESET Endpoint Security voltará para o servidor primário. A configuração de dois perfis de servidor de administração remota é mais adequada para clientes que se conectam tanto da rede local como de fora da rede.

**Endereço do servidor** - especifique o nome DNS ou o endereço IP do servidor que executa o ERA Server.

**Porta** - este campo contém uma porta de servidor predefinida usada na conexão. Recomendamos que você deixe a porta padrão definida como 2222.

Se o ESET Remote Administrator exigir a autenticação por senha, selecione a opção **O servidor de administração remota requer autenticação** e digite sua senha no campo **Senha**.

**OBSERVAÇÃO:** Para obter orientação adicional sobre como gerenciar sua rede usando o ESET Remote Administrator, consulte o Manual de Instalação e o Guia do Usuário do ESET Remote Administrator (esse documento talvez não esteja disponível em seu idioma).

# 9. Atualização

O ESET Endpoint Security pode ser facilmente atualizado para a versão de produto mais recente, a fim de garantir que seu dispositivo móvel seja protegido em relação às ameaças mais recentes e ataques mal-intencionados. Se você receber uma notificação de que uma nova versão do ESET Endpoint Security está disponível para download, a ESET recomenda que você a instale assim que possível.

Por padrão, o ESET Endpoint Security é instalado com uma tarefa de atualização a fim de garantir que o programa seja atualizado regularmente. Para executar a atualização manualmente, toque em **Atualizar agora** .

**Configurações**

A opção **Atualização automática** permite definir o intervalo de tempo para o download automático das atualizações do banco de dados de vírus.

**OBSERVAÇÃO:** Para evitar a utilização desnecessária da largura de banda, as atualizações são lançadas apenas quando necessário, ou seja, quando surge uma nova ameaça. Embora as atualizações sejam fornecidas gratuitamente com sua licença ativa, a operadora poderá cobrar pela transferência de dados.

# 10. Senha

A senha de segurança protege suas configurações contra acesso não autorizado. Uma senha é necessária para:

- acessar recursos do ESET Endpoint Security protegidos por senha (Antivírus, Antispam, Antifurto e Auditoria de segurança)
- acessar o telefone depois que ele for bloqueado
- enviar comandos por SMS para o dispositivo
- desinstalar o ESET Endpoint Security.

**OBSERVAÇÃO:** A proteção contra desinstalação está disponível apenas no Android 2.2 e em versões posteriores.

Para definir uma nova senha de segurança, digite-a nos campos **Senha** e **Digite novamente a senha**. A opção **Lembrete de senha** (quando configurada) exibe uma dica para o caso de você não lembrar sua senha.

**IMPORTANTE:** Escolha sua senha com cautela, pois ela será necessária para desbloquear o dispositivo ou desinstalar o ESET Endpoint Security.

Na guia **Aplicar a**, é possível especificar quais módulos serão protegidos pela senha.

Se você esquecer sua senha, poderá enviar um SMS para seu número a partir do celular salvo na lista **Contatos do administrador**. Esse SMS deve ter o seguinte formato:
*eset remote reset*
Sua senha será redefinida.

# 11. Solução de problemas e suporte

## 11.1 Solução de problemas

O ESET Endpoint Security conta com recursos avançados de registro em log que ajudam a diagnosticar possíveis problemas técnicos. Antes de entrar em contato com o Atendimento ao cliente da ESET, recomendamos que você pesquise uma possível solução na Base de conhecimento da ESET. Caso ainda precise entrar em contato com o Atendimento ao cliente da ESET, siga as etapas a seguir:

1. Vá para o menu principal do ESET Endpoint Security, pressione o botão **MENU** e toque em **Configurações de logs**.
2. Selecione um componente apropriado do programa ao qual o problema está relacionado.
3. Replique o problema. As informações serão gravadas em um arquivo de log do aplicativo.
4. Vá para o menu principal do ESET Endpoint Security, pressione o botão **MENU** e toque em **Atendimento ao Cliente**.
5. Caso não encontre uma solução na Base de conhecimento, toque em **Continuar**.
6. Preencha todos os detalhes e toque em **Enviar** na parte inferior da tela. Certifique-se de que a opção **Log do aplicativo** esteja selecionada (padrão).

## 11.2 Suporte técnico

Nossos especialistas de atendimento ao cliente estão disponíveis para ajudar caso você precise de assistência administrativa ou suporte técnico relacionado ao ESET Endpoint Security ou a outro produto de segurança ESET.

Para obter respostas a perguntas frequentes, acesse a Base de conhecimento da ESET no endereço:
*http://kb.eset.com/android*

A Base de conhecimento traz muitas informações úteis sobre como solucionar os problemas mais comuns. Elas podem ser acessadas com facilidade por categorias ou uma ferramenta de pesquisa avançada.

Para entrar em contato com o Atendimento ao Cliente da ESET, use a solicitação de suporte disponível no endereço:
*http://www.eset.com.br/support/contact*

Para enviar uma solicitação de suporte diretamente de seu celular, vá para o menu principal do ESET Endpoint Security, pressione o botão **MENU** e toque em **Atendimento ao cliente**. Preencha todos os campos obrigatórios. Para incluir um **Log do aplicativo** completo, siga as etapas descritas na seção Solução de problemas 11.